Amendments to the Specification

Please delete the entire paragraph found on page 4, between lines 9 - 29.

Please delete the entire paragraph found on page 5, between lines 1 – 12.

Please insert the following new paragraph on page 4, following line 8:

In one aspect, the present invention provides a method for verifying a signature for a message *m* in a data communication system, established between a sender and a recipient, said sender generating masked signature components (r, s, c), where r is an integer derived from a coordinate of a first short term public key kP, s is a signature component derived by binding a second short term private key, the message *m* and short and long term private keys, and c is a second signature component obtained by combining said first and second short term private keys, the method comprising the steps of having a verifier: obtain a pair of signature components $(\bar{s}, r)$, the component $\bar{s}$ being derived from first and second signature components generated by a signor; recovering a coordinate pair (x_1, y_1) corresponding to said first short term public key kP using the pair $(\bar{s}, r)$ and the message *m*; calculate a signature component r' from one of the coordinate pairs; and verify the signature if $r' = r$.